ABSTRACT

An Active Filtering proxy filters electronic junk mail (also known as spam, bulk mail, or advertising) received at a Message Transfer Agent from remote Internet hosts using the Simple Mail Transfer Protocol (SMTP). The proxy actively probes remote hosts that attempt to send mail to the protected mail server in order to identify dialup PCs, open relays, and forged email. The system provides multiple layers of defense including: connect-time filtering based on IP address, identification of dialup PCs attempting to send mail, testing for permissive (open) relays, testing for validity of the sender's address, and message header filtering. If a message passes through all relevant layers, it is delivered directly to all recipients. A recipient whitelist database permits the user or system administrator to identify particular senders and/or domains as acceptable. If one or more recipients have agreed to receive mail from the sender, the message is delivered to those recipients and rejected or quarantined for the remainder of the recipients. The system includes a quarantine mechanism for messages rejected by Active Filtering that permits administrators and users to review intercepted messages and forward selected messages to the local mailhost for delivery.